IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) An apparatus for generating pseudorandom sequences comprising:

a two-dimensional cellular automata random number generator ~~of a first type~~ configured to generate a first sequence ~~with a first predetermined randomness and a first predetermined period~~;

a 2-by-L cellular automata random number generator ~~of a second type~~ configured to generate a second sequence ~~with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period~~;

a controllable cellular automata random number generator configured to generate a third sequence by determining cell states based on a corresponding cell control word and/or a corresponding rule control word, wherein the cell control word is generated by the 2-by-L cellular automata random number generator and the rule control word is generated by the two-dimensional cellular automata random number generator; ~~and~~

adders configured to perform bit-to-bit mod2 sum of the first, second and third sequences ~~and the second sequences~~;

a first block configured to perform a nonlinear mapping on the summation results from the adders; and

a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as a pseudorandom sequence.

2-5. (Canceled)

6. (Currently Amended) The apparatus according to claim 1 [[5]], wherein:

each of the first and second blocks include ~~includes~~ at least one nonlinear function.

7. (Currently Amended) The apparatus according to claim 1 [[5]], wherein:

the second block includes at least one look-up table for nonlinear mapping based on the Latin squares.

8. (Currently Amended) An apparatus for performing cryptographic processing comprising:

a cryptographic processor configured to encrypt ~~for encrypting~~ data using pseudorandom sequences; and

a pseudorandom sequence generator configured to generate ~~for generating~~ pseudorandom sequences, wherein the pseudorandom number generator is configured to include the apparatus according to claim 1.

9. (Currently Amended) A method for generating pseudorandom sequences using cellular automata in a pseudorandom sequence generator comprising:

generating, at a two-dimensional cellular automata random number generator ~~of a first type~~, a first sequence ~~with a first predetermined randomness and a first predetermined period~~;

generating, at a 2-by-L cellular automata random number generator ~~of a second type~~, a second sequence ~~with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period~~;

generating, at a controllable cellular automata random number generator, a third sequence by determining cell states based on a corresponding cell control word and/or a

corresponding rule control word, wherein the cell control word is generated by the 2-by-L cellular automata random number generator and the rule control word is generated by the two-dimensional cellular automata random number generator; ~~and~~

performing, at adders ~~an adder~~, bit-to-bit mod2 sum of the first, second and third sequences ~~and the second sequences~~;

performing, at a first block, a nonlinear mapping on the summation results from the adders; and

performing, at a second block, a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as a pseudorandom sequence.

10. (Canceled)

11. (Currently Amended) A non-transitory computer readable recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the method comprising:

generating, by a two-dimensional cellular automata random number generator, a first sequence ~~with a first predetermined randomness and a first predetermined period~~;

generating, by a 2-by-L cellular automata random number generator, a second sequence ~~with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period~~;

generating, by a controllable cellular automata random number generator, a third sequence by determining cell states based on a corresponding cell control word and/or a corresponding rule control word, wherein the cell control word is generated by the 2-by-L cellular automata random number generator and the rule control word is generated by the two-dimensional cellular automata random number generator; and

performing bit-to-bit mod2 sum of the first, second and third sequences ~~and the second sequences~~;

performing a nonlinear mapping on the summation results; and

performing a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as a pseudorandom sequence.

12. (Currently Amended) The apparatus according to claim 1, wherein the first sequence generated by the two-dimensional cellular automata random number generator ~~of a first type~~ satisfies the DIEHARD test.

13. (Currently Amended) The apparatus according to claim 1 [[2]], wherein the two-dimensional cellular automata random number generator ~~of a first type~~ generates two-dimensional cellular automata including 64 cells.

14. (Currently Amended) The apparatus according to claim 1 [[2]], wherein the two-dimensional cellular automata random number generator ~~of a first type~~ generates two-dimensional cellular automata arranged in an 8x8 array.

15. (Previously Presented) The apparatus according to claim 1, further comprising:

a buffer configured to buffer results of the bit-to-bit mod2 sum.

16. (Currently Amended) The apparatus according to claim 1 [[2]], wherein the adders output pseudorandom sequences with a controllable period.

17. (Currently Amended) The apparatus according to claim 1 [[3]], wherein the controllable cellular automata random number generator ~~of the third type~~ includes a plurality of cell units.

18. (Currently Amended) The method for generating pseudorandom sequences according to claim 9, further comprising: ~~comprising~~

generating a key for cryptographic processing based on the generated pseudorandom sequences.

19. (Currently Amended) The method for generating pseudorandom sequences according to claim 9, further comprising: ~~comprising~~

interfacing with an external device.

20. (Previously Presented) The method for generating pseudorandom sequences according to claim 19, wherein the interfacing includes inputting information designating the key to be used and outputting encrypted text data based on the key.